REMARKS

Status of the application

Claims 1-2, 14-29, 31-34, 37-38, and 41-48 were examined and stand rejected in view of prior art. The claims have been amended to further Applicant's claimed invention. Reexamination and reconsideration are respectfully requested.

General

Claims 1 and 18 were objected to for reciting an informality. Appropriate correction has been made.

Prior art rejections

1. Section 102 rejection

Claims 1-12, 14, 18-19, 31, 37-38 and 41-48 are rejected under 35 U.S.C. § 102(a) as allegedly being anticipated by Jones et al. WIPO Pub. WO 03/030483 (hereinafter "Jones"). The rejection is respectfully traversed.

Claim 1 now recites:

> 1. A computer-implemented method for improving service accounting in a network, the method comprising the steps of:
> in response to a first Authentication, Authorization, and Accounting (AAA) server
> receiving a request to authorize a client,
> said first server obtaining an accounting record for the client,
> said first server authorizing said client based on said accounting record, and
> **said first server sending a Remote Authentication Dial In User Service protocol (RADIUS) access accept message that includes the accounting record within the access accept message;**
> **causing the accounting record to be logged;**
> a second AAA server receiving a RADIUS start session message that includes the accounting record within the start session message.

(Emphasis added.) At least the above-bolded portion of claim 1 is not taught or suggested by Jones.

Jones does not send an access accept message containing an accounting record.

In rejecting claim 1, the present Office Action contends that Jones describes the feature of claim 1 reciting "said first server sending a Remote Authentication Dial In User Service protocol (RADIUS) access accept message that includes the accounting record within the access

accept message". Applicant disagrees. However, to resolve any potential ambiguity of the previously presented set of claims, claim 1 is amended to recite (shown in amended form):

in response to a first Authentication, Authorization, and Accounting (AAA) server receiving a request to authorize a client,
said first server obtaining an accounting record for the client,
said first server authorizing said client based on said accounting record, and
said first server sending a Remote Authentication Dial In User Service protocol (RADIUS) access accept message that includes ~~at least a portion of~~ the accounting record within the access accept message;
causing ~~at least a portion~~ the accounting record to be logged;
a second AAA server receiving a RADIUS start session message that includes ~~at least a portion~~ the accounting record within the start session message.

As shown by the foregoing features of amended claim 1, the accounting record sent by the AAA server in the access accept message is used as a basis for authorizing the client. As noted in the background of Applicant's specification, information that an AAA server uses to make an authorization decision may be useful for creating richer log and audit trails (See Applicant's specification, paragraph [0008]). Applicant's approach of claim 1 allows the creation of richer logs and audit trails in a manner that is more efficient than is possible with the approaches of the prior art.

For example, in an embodiment of claim 1 in which the first AAA server and the second AAA server are the same AAA server, the AAA server may wish to log the accounting record in response to receiving the start session message. Prior approaches **including Jones** require the AAA server to cache the accounting record between sending the access accept message and receiving the start session message. The problem with caching the accounting record is that caching the data limits load balancing of AAA servers and would require the AAA server to keep state for each client session. That is, if the AAA server cached all required information, then the RADIUS accounting messages, also known as Call Data Records (CDR), would then have to be routed through the same AAA server that performed the authentication (See Applicant's specification, paragraph [0013]).

In an embodiment of claim 1 in which the first AAA server and the second AAA server are different load-balanced AAA servers, prior approaches for creating richer log and audit trails require a load-balanced AAA server to re-obtain the accounting record, perhaps from an external resource server, in response to receiving the start session message. The problem with re-

obtaining the accounting record is that it is inefficient and can create excessive load on an external resource server.

To address these and other problems of the prior art, Applicant's invention of claim 1 sends the accounting record **that was used to authorize a client** in a RADIUS access accept message and receives the accounting record in a subsequent RADIUS start session message. Applicant's approach of claim 1 allows load balanced AAA server to create richer logs and audit trails without having to re-obtain accounting records from external resource servers. Applicant's approach of claim 1 also eliminates the need for an AAA server to cache accounting records in order to create richer logs and audit trails. Support for the amendments to claim 1 can be found in Applicant's specification at paragraph [0042] and at paragraph [0044].

Turning to the cited art, Jones' stateful RADIUS server does not send data used to authorize a client in an access accept message. The RADIUS server in Jones does send a session key in an access accept message. For example, Jones at col. 11, lines 29-33 states:

> In the context of this example the stateful RADIUS server 62 locates the data session on PDSN A 58 in its cache and constructs a Class attribute containing the IP address of PDSN A 58 and the Acct-Session-Id of the data session on PDSN A 58. This Class attribute is appended to the access accept message returned to PDSN B 82 at step 102.

However, the IP address of the PDSN and the Acct-Session-Id (which Jones also refers to as a "session key") are not accounting records. Jones' session key is not an accounting record because Jones' RADIUS server does not use the session key to authorize a client. That is, Jones' RADIUS server does not use the session key to determine whether a client should or should not have access to a requested resource. Rather, the session key in Jones is used by the RADIUS server to track a mobile device's packet-data sessions, but is not used a basis for authorizing the mobile device.

As clearly described in Jones, the RADIUS server in Jones authorizes mobile devices independent of the session key sent in access accept messages. For example, Jones at col. 11, lines 26-33 states:

> On receipt of the access request message, **the stateful RADIUS server 62 performs the usual authentication and authorization process, then** checks for the existence of a pre-existing data session from the same mobile node 54', at step 100. In the context of this example the stateful RADIUS server 62 locates the data session on PDSN A 58 in its cache and constructs a Class attribute containing the IP address of PDSN A 58 and the Acct-Session-Id of the data session on PDSN A 58. This Class attribute is appended to the access accept message returned to PDSN B 82 at step 102.

(Emphasis added.) As clear from the above cited portion, the session key is used by the RADIUS server only **after** the RADIUS server has performed the "usual authentication and authorization process". Jones also states at col. 6, lines 19-21:

> It should be noted that a new session key is not assigned at the time of authentication/authorization since confirmation of the session creation only occurs on receipt of the accounting start message.

The above-cited portion of Jones also makes clear that Jones' RADIUS server could not possibly authorize a client based on the session key since the session key is not created at the time of authentication/authorization.

In sum, nothing in Jones teaches or suggests using the session key as a basis for authorization. Since what Jones sends in the access accept message is not used as a basis for authorization, Jones does not satisfy the following feature of Applicant's claim 1:

> in response to a first Authentication, Authorization, and Accounting (AAA) server
> receiving a request to authorize a client,
> said first server obtaining an accounting record for the client,
> said first server authorizing said client based on said accounting record, and
> said first server sending a Remote Authentication Dial In User Service protocol (RADIUS) access accept message that includes the accounting record within the access accept message;

Jones is not about logging.

Jones has no mention of a "log" or "logging" that could be relevant to the feature of Applicant's claim 1 reciting "causing the accounting record to be logged". This is unsurprising because Jones is not directed to techniques for logging within a network. Rather, Jones is about addressing a very specific problem that occurs in some mobile wireless data networks. Specifically, Jones addresses a "handoff" problem caused by a mobile device moving between two stationary radio networks when the mobile device is in a "dormant state" (see Jones, col. 1, line 31 – col. 2, line 21.) However, Jones does not describe its PDSNs or RADIUS server performing any sort of logging during this handoff procedure.

In rejecting claim 1, the Office Action cites to Jones at col. 10, lines 23-25 for the prospect that it satisfies the logging aspects of Applicant's claim 1. The cited portion of Jones states, in its entirety:

> First, at step 84, the PDSN A 58 transmits an access request message to the stateful RADIUS server 62. The stateful RADIUS server 62 then performs some manner of

lookup at step 85 to establish whether the communication should be allowed.

As with the rest of Jones, the cited portion says nothing about a "log" or "logging". Jones does describe the RAIDUS server creating a session record in a cache (see e.g., Jones, col. 10, lines 31-33.) However, one skilled in the art would not equate storing data in a cache with logging data to a log. One skilled in the art would not do so at least because caching data implies storing data for a relatively short period of time, perhaps only in a volatile memory; while logging implies storing data for a relatively long period of time, perhaps permanently and on a non-volatile storage medium. Thus, one skilled in the art would not equate Applicant's logging with Jones' caching.

Based on the foregoing, Applicant respectfully submits that claim 1 is allowable over Jones. Applicant's claim 1 involves an AAA server sending, in a RADIUS access accept message, an accounting record that was used as a basis for authorizing a client. Jones' requirement of caching the session data at the RADIUS server requires that all RADIUS accounting messages by routed through the same RADIUS server. Nothing in Jones describes using its session key as a basis for authorizing a client. At best then, Jones is merely duplicative of what Applicant's have already disclosed in the Background of their Specification. Further, Jones is not about logging in a data network. Therefore, Applicant's claim 1 is not anticipated by Jones.

Applicant's claim 18 recites similar features to those recited in claim 1 and is allowable over Jones for the same reasons.

2. Remaining claims

The pending claims not discussed so far are dependant claims that depend on an independent claim that is discussed above. Because each dependant claim includes the features of claims upon which they depend, the dependant claims are patentable for at least those reasons the claims upon which the dependant claims depend are patentable. Removal of the rejections with respect to the dependant claims and allowance of the dependant claims is respectfully requested. In addition, the dependent claims introduce additional features that independently render them patentable. Due to the fundamental differences already identified, a separate discussion of those features is not included at this time.

Conclusion

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a check for the petition for extension of time fee and other applicable fees is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Dated: August 4, 2009

/AdamCStone#60531/
Adam C. Stone
Reg. No. 60,531

2055 Gateway Place Suite 550
San Jose, California 95110-1093
Telephone No.: (408) 414-1080
Facsimile No.: (408) 414-1076